Cloudlet-based privacy preserving for securing medical data In Cloud by using homomorpic encryption technics.

Chaitanya kumar
Mtech, Dept of CSE, SNIST, Hyderabad, Telangana, India
Email: chaitanyakumar86990@gmail.com
Doddi Srilatha
Assistant professor, Dept of CSE, SNIST, Hyderabad, Telangana, India
Email: Doddisrilatha@gmail.com

Abstract— Cloud computing is a model that provides physical and logical resources over the Internet. Cloud computing attracts the government, IT organizations, Individual users especially cloud computing is mostly used in Health care organization for storing and sharing the patient's health care information. Practitioners remotely monitor the patient health information through the wearable devices attach to the patient body. By using particular equipment together with cloudlet knowledge it has became a major agenda to provide better medical availability. The handling series with health information possess information gathering, information loading (storing) and information division, etc. Cloud is predominantly used in health care organizations for storing and sharing the patients' health information among practitioners and patients. The information can be even accessed by unauthorized (malicious) users to steal or to misuse the patient information. Data security and sharing of patient records are key challenging issues in the cloud to be addressed. Hence, as part of the project work, we try to develop a solution to address this issue in this proposed project, we address these issues by using

– Homomorphic Encryption, for secure storage of medical data in cloud and

– Trust Level Mechanism, based on similarity of patient diseases for better sharing of medical data between users.

Index Terms— privacy protection, data sharing, Homomorphic Encryption, Trust Level Mechanism, healthcare.

1 Introduction

THIS Cloud computing denotes a fresh method, now selected cases an additional price effective way, of transporting enterprise IT. For example, totally main disruptive modifications in knowledge and advanced features, cloud computing denotes a correct implementation on Net completion , and it doesn't do only a shifting the corporate examples and the manner IT organization is being transported and spent, but also the fundamental construction of how we grow, arrange, run and transport implementation.

1.1 cloud computing Why it is used to medical Requirement?

Several medical care workers and insurance corporations nowadays have approved some method of electronic health information schemes, though maximum of them collection health information in central records in the structure of electronic accounts. Naturally, a sufferer might have several, medical care workers, containing key care nurses, therapists, experts, physicians, and additional medical specialists. In along with this, a sufferer can utilize many medical care insurance corporations for dissimilar kinds of insurances, such as health, dental, and so forward. Now, both workers usually must its own cloud for electronic health registers. Splitting data among medical experts across executive limits is decoded to allocation data among electronic health registers systems. The electronic information distribution among changed electronic health registers systems is known electronic health records (EHRs). The internal work and allocation within different Electronic health registers has been very poor. Price and less usage have been named as the major problems to acceptance of medical IT, especially Electronic Health Records (EHR) systems. Information computing offers a nice IT stage to modified down the price of EHR systems in terms of both ownership and IT care loads for several health follows.

It is generally known that cloud implementation plus open values are vital foundations for updating medical care whether it will be used for keeping medical histories, observing of patients, handling sicknesses and cares extra capably and healthy, or partnership with peers and investigation of records. Several expect that handling medical care requests with clouds will sort new adjustment in the system we do medical care nowadays. Allowing the contact to medical care universal not only will benefit us increase medical care as our files will always be available from everyplace at whichever you want, but also it benefits decreases the prices extremely. a important phase for the achievement of medical care into the database is the full understanding and the real application of safety and protection in cloud computing.

1.2 Guarding plus preotectcing Problems in

medical data

Study with the several safety problems nearby medical care Data schemes have been heated finished the previous rare years. ISO/TS 18308 standard provides the descriptions of safety and confidentiality problem for EHR [5]. The Working Cluster 4 of International Medical Informatics Association (IMIA) was set up to explore the problems of records safety and confidence inside the medical care location. Its work to date has mostly focused on safety in EHR interacted schemes and shared safety explanations for shared sufferer information [6]. The European AIM/SEISMED (Advanced Informatics in Medicine/Secure Environment for Information Systems in Medicine) scheme is introduced to speech a varied band of security issues within medical care then delivers useful rules for protected medical care launch [7,8,9]. "Would make a private medical file that sufferer, specialists and additional medical care workers could securely contact over the Internet no problem anywhere a sufferer is pursuing health care."

Wearable devices, health care big data, cloud computing etc. the patient can send his health records to the nearby doctor and a communication can be made among doctor and a patient. But the sensitive records can be leaked or changed over by the third person or the attacker and hence this causes safety problem. Via the cloud computing much of the data can be held in the clouds that contain cloudlets and the protected clouds. The major drawback here is the security and privacy from unkind attacks. Taking attention of above problem, this publication provides information about cloudlet health care system (reference K. Hung). The Gathering records from wearable devices are transferred to the close cloudlets from where it is further conducted to the confident clouds from where doctors will access the records and analyze the disease. The privacy protection is spread into three stages. In the first stage the records of user's health together via wearable devices is transferred to the nearby cloudlets. Transmission of this health information needs to be safe a lot. Next, the records from the cloudlet are transmitted to the safe cloud where the third stage the data is divided into different types and corresponding security is provided.

2 LITERATURE SURVEY

2.1 Secure cloud storage of data

Abstract: Cloud computing is one of the demanding and secure technology which is widely popular in IT industry across the globe because of its security reasons and amount of data without losing data. We can access the data from any where in the world so, let's get started with how does this mechanism work on mobile phones.

Existing system: Mobile phones contains many important data which requires protection from unauthenticated sources even if the phone lost or damaged. So as back up option we can store the data in computers(server) or pen drives (hard disk). But it is not secure as a computer network can be hacked or infected by some virus during retrieval or transmission of data.

Proposed system: Data is stored in such a way that we can upload/download/save the files through cloud computing in mobile phones. It needs authentication to access the data. So, we generate an unique key every time we log on to the system for accessing the unique key can be caused as token key. It is used for authentication to store the keys. We use organization, if the data matches, we can access the data, in the way it provides security to the user's data from threats. The token key is encrypted and send to the users who are in the privilege its. So, the key can be decrypted, and the data can be accessed.

2.2 Cloudlet mesh for securing mobile clouds from intrusions and network attacks

Abstract: This publication provides a new cloudlet mesh for guarding implementation to provide trusted mobile data base computing. The cloudlet mesh is Wi-Fi or mobile attached to the source. This security framework established a cyber trust protection to fight opposite to intrusions to away database. Prevent malwares on mobile database resources and pause unauthorized access in other cloud.

Existing system: This publication attempts to remove the problem with the help of a mesh of database to implement the needed authentication, authorization and encrypt operations to provide a trusted mobile computing. This security framework to fight opposite intrusions to distance clouds, prevent malwares attacks on mobile database resources, and stop unauthorized entrance of shared datasets in removing the cloud.

Proposed system: To guard mobile devices from malware attacks, we implement the remote cloud for data extreme filtering and updating the attack signature cloud. The cloud designed security system works as an intellectual firewall or IDS to guard mobile devices within range of the underlying Wi-Fi mesh.

- improve chain establishment between mobile devices, the database mesh and remote source.
- virus signature scanning and update with automated virus/spam filter and removal.
- real time filtering or removal of malicious attacks or intrusion help trusted model.

2.3 Wireless Patient Monitoring System

Abstract: Most of the people who go to hospitals requires nurses to monitor the test reports before consulting the doctor for prescribed medications. But unfortunately, there are less nurses to guide patients while the latter is rapidly increasing exponentially. Then in that case, there is a kind of solution which does not need patients to stay on beds for undergoing tests. Let's discuss what it is all about Some examples of this technology include blue code and visi mobile device technology.

proposed system -blue was designed with an intention to keep track of individual patients and data transfer records by using pulse ox meter. Visi mobile device can be used to monitor the heart beat -blood pleasure, ECG, respiration and body temperature. Code blue technology can keep track of the data in records while visi mobile device technology cannot.

2.4 Advanced Protection for Patient Information in Medical Database

Abstract: - In most of the healthier the officers (or) specialists will be having any access to information which is not recommended. There comes the privacy concern issue to safeguard this data against spam users. In order to safe guard this data can be achieved by introducing cryptosystem which improves confidentiality of data which makes the data under certain lock. And reduces the access. So here by using this attempt high security for sufferer's vital information can be provided. Here it is implemented with the help cryptography as the main implementation.

Work and use: - This implementation provides an effective process to implement a well secured mechanism for sufferer state irrespective of remaining medical solutions. This uses pailer & homomorphic encryption for sufferer's health type there by provided safe guard to data.

3 STRUCTURE CONTEXT

In hospitals, data posses of vital sufferer information, which is protected in devices and provides with privacy of that particular data are vital. The information of those details is stored with lot of security.

1. In the publication we study about cloudlet base medical system. The information possessed from equipment are processed to supporting cloudlet. The information is next sent to required cloud where the specialists can acquire it and prepare for treatment as per data process chain. The guarding of information is in 3 stages.

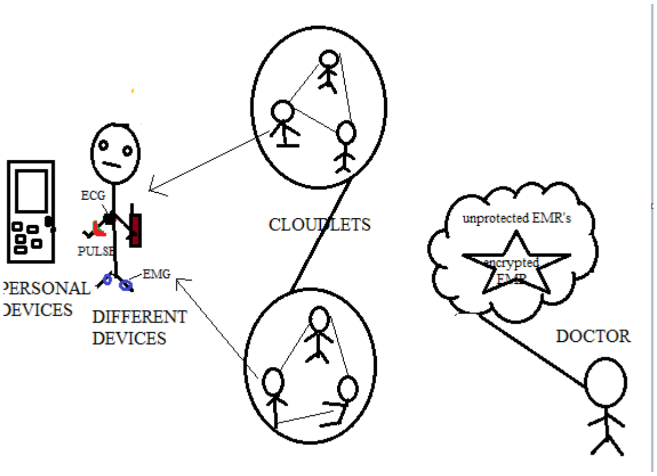
1.1. In the earliest process sufferer important symptoms by equipment as the below figure provides to nearest close gateway of cloudlet. Here data security is main concern.

1.2. In the next stage suffers data will next processed for remote cloud into database. A cloudlet is created with limited secured electronic devices whose provider may require or transform some preformed information data. so, both protecting, and information processed are discussed here.

1.3. Mainly we utilize trust level mechanism to calculate belief fetch between sufferers to find spited information or not. Checks the sufferer's health data protected in database, we define this health information into separate types the corresponding information policy.

2. cloudlet is obtained by some number of electronic mobile whose holder may need or split information. Then both security and information are discussed here.

3. We adapt homomorphic encryption for information security while transmitting to cloudlet. The proposed system can prevent the vital data from any malwares. Together with three stages with information protection.



System framework

4 CLOUD BASED DATA PROTECTION

Here this publication we discuss the data security and split of patients records and its privacy. Early we provide to description procedure regains sufferer private information. It safe guards sensitive data sensitive data loss problem or to prevent patient private information changed or stolen by some suspicious user through sending. Next we present the trust based model of patients who need to contact patient hospitals records. Thus we can give different patients phases of different approvals for records acquirement.

4.1 Description at user end:

Here the Description includes the entire process flow at from the devices to outcome at the user end. i.e. from devices to cloudlet. The process includes the vital information of the sufferer. Where as vital information includes sufferer's cognitive data like heart rate, blood pressure and electro cardiograph (ECG). All this vital information from sufferer and collected with their respective devices. Now all this information from sufferer is now processed to an application named cloudlet. Cloudlet is a software application which is used to store private data. While processing the data from sufferer devices to cloudlet we use a technique named Homomorphic encryption. Here the main purpose of using this Homomorphic encryption is to achieve more secure storage of medical information in cloud. Homomorphic encryption is form of encryption allows computation on cipher texts, generate an encrypted result which, when decrypt matches the result of operation performed on plain text. This Homomorphic encryption internally uses paillier algorithm for successful of the data available.

4.2 sufferer information sharing in cloudlet:

The main purpose to have sharing of details between sufferers to make easy way of sorting between same kind of sufferers. This result in essay identification with in less time in an efficient manner. here we are proposing strategically sharing of data between cloudlet using encrypted methods which doesn't include sufferer activates. As we discussed above process let us check the process. for our understanding purpose here, we assuming two patients p and p1. When p asked a authority to check of p1 that indicates one patient is shares information with p1 then work by authority will be processer in two steps.

Step – 1, similarity (it includes disease information) of both sufferers well the similarity can be of 3 levels like namely low, moderate and high.
Step -2, this involves the description of trust level both sufferers i.e., by using reputation of both users as an input from step 1 i.e., reputation like good, bad and average by utilizing this trust model for obtaining the permission whether to share or not to shape data. i.e., if the Trust level between the users is high, we can access the permission to share information.

Later finding patients belief measure, we cold justice if we can belief patient(p) on available max rack fixed on patient(p1). when the belief measure is similar to more than threshold rate, before patient(p) is can be trusted so management will split the (p1) data to user p. if belief measure is in lesser amount then threshold then patient p is hard to belief and authority can reject the request of patient.

4.3 information security in cloud:

The main purpose to perform security operators to information is to have a secure data and which cannot be accessed by others. As we know the data regarding patient's treatment and records of diagnosis are stored in many separate files. To store the vast data that resembles the patient information we are using cloud which reduces ambiguity. This process of saving data in cloud reduces cost and easy way for doctors to treat and analyze diseases. On the other hand, it will provide lot more security which reduces the leakage of personnel information. As we using the encrypted technique which the described user with proper credentials can access the data regarding the user which improves security and cannot be accessed by uncertified or unlicensed user. This process of providing security with cloudlet application is in 3 ways.

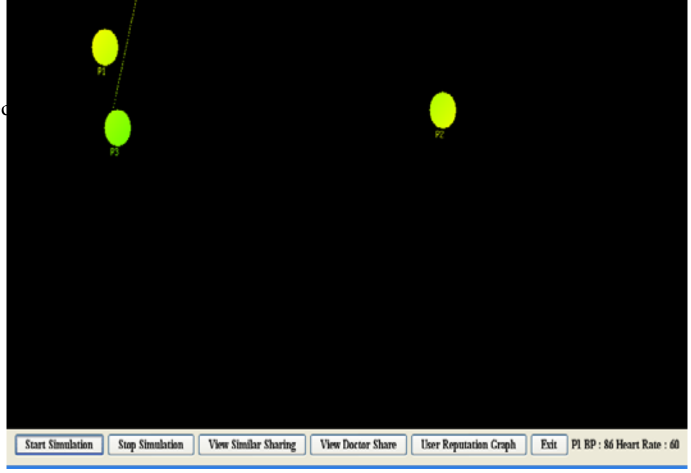
a) In first Phase the patient with particular ID with email. Ph no and address.
b) In second phase it saves patient details with their particular Zip code, Data of Birth and Gender.
c) Finally, in last phase saves information of the disease and diagnostics.

Finally, Among the three phases the third phase is provides with much security. By this way of using encrypted data we can achieve secured patient information in an efficient and secured manner and usage of cloudlet helps in easy way to access information when compared to existing application. This provides a lot more compatibility and reduces ambiguity between patients with efficient manner.

5 CLOUD LET BASED SECURITY:

5.1 sending to cloudlet:

here in this graph, as here the graph provided as preview for the storing the patient data into the cloud.

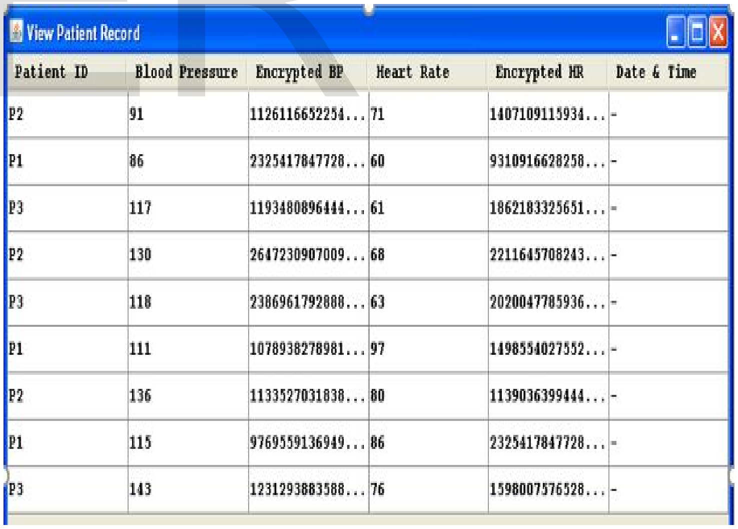


P1 BP : 86 Heart Rate : 60

now the above simulation shows what process exactly takes place. In the beginning when the simulation is started process by clicking on start button. The patient data from cloud be encrypted by using Homomorphic technique and will be added into nearest cloudlet. The same process will be repeated for ball the active patients i.e., patient attached with variables devices like BP, HR meter etc. and will check all the data and send it to nearest cloudlet. This process of storing data into cloudlet by encrypted makes it more secure and increases efficiency.

5.2 data encryption process:

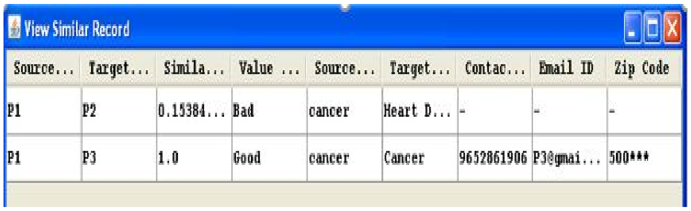
Below screenshot show the how data secure detailed process of patient Records.


View Patient Record

Patient ID	Blood Pressure	Encrypted BP	Heart Rate	Encrypted HR	Date & Time
P2	91	1126116652254...	71	1407109115934...	-
P1	86	2325417847728...	60	9310916628258...	-
P3	117	1193480896444...	61	1862183325651...	-
P2	130	2647230907009...	68	2211645708243...	-
P3	118	2386961792888...	63	2020047785936...	-
P1	111	1078938278981...	97	1498554027552...	-
P2	136	1133527031838...	80	1139036399444...	-
P1	115	9769559136949...	86	2325417847728...	-
P3	143	1231293883588...	76	1598007576528...	-

Example - The patient with Blood pressure with 91 their ID along with heart rate. this entire information is encrypted and seat to cloudlet. The blood pressure 91 will be encrypted to particular encrypted ID of Big Integer Number(9512458796251255) and similarly for heart rate.

5.3 Similarity process:

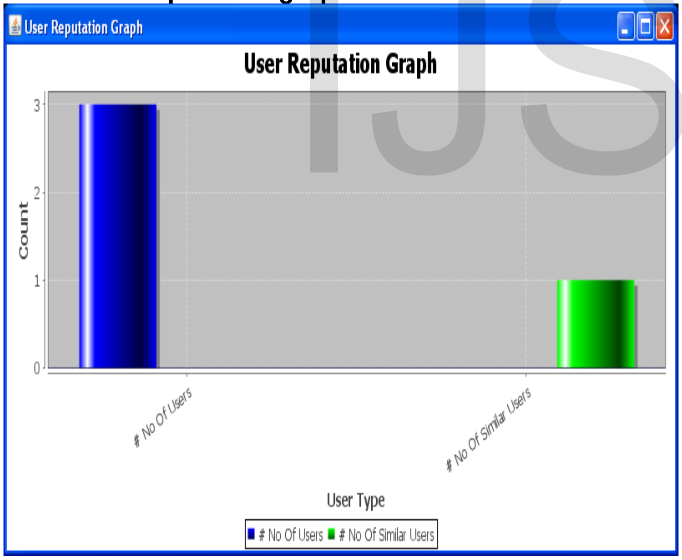


View Similar Record

Source...	Target...	Simila...	Value ...	Source...	Target...	Contac...	Email ID	Zip Code
P1	P2	0.15384...	Bad	cancer	Heart D...	-	-	-
P1	P3	1.0	Good	cancer	Cancer	9652861906	P3@gmai...	500***

The process of accessing multiple patient records is shows in the above simulation process. Whenever when we require to accessing the suffers with same disorder it can be accessed by using the cloudlet. as the suffered Id entered as an input it will compare the defectives (or) disease of the entered suffered with all the patient with relative deficiency. The main comparison will be based on the Trust Level Mechanism. Here it compares the record with other records and then retrieves all corresponding patients of the same disorder. if the trust level between the two compared suffers reaches a good level then it will display the records if not it do not display the records. Let's see an example if a patient have a disease and symptoms and required to hare the person with same deficiency like fever there comes the Trust Level Mechanism and provides the data. if the Trust level of patient1 with fever and has the same problems with patient1 then data of patient2 will displayed. If it does not match it does not match it does not show the Patient information.

5.4 Userl repulation graph:



However at last in order to attain the complete patients information and get the details we can take help of a graph. Here in the graph we are using data of both sufferers count and number of sufferers. The user reputation graph provides complete details of patients count vs. similar disease. In the graph we have data from which the blue column indicates the patients count where as green column indicates the sufferers with similar faults. If the Trust level mechanism results good, we can see the increment in green column. The main purpose for representing sufferers' records in graphical manner to have easy access of sufferer's details.

6 Future WORK:

In this cloudlet-based preserving for securing medical data in cloud by using homomorphic encryption techniques, we are using high encryption technique which makes the data to be more safe and secure. The main advantages of using this technique it have the easy way of communication between patient and doctors. which makes it a concise way when compared to other process. Here in this as we are using Homomorphic encryption which enables meaningful computations on encrypted data without decrypting it. Here we have limited the usage of IDE, whether in future if we have any indication of any malware which makes a problem in application deployment, so usage of IDE will makes it a perfect encryption without flow.

7 Conclusion:

This method we are able to solve the privacy protection of user whose information is shared in large medical data with the help of Cloudlet and remote cloud. This can be performed mostly compared to existence methods.

By using the cloudlet and encrypted data by using Homomorphic encryption technique we can achieve data security and sharing can be done which are the major challenges. As here we are using trust level mechanism which access our way easy to compare the data between users and sharing .

Finally by remote cloud the data present can be protected with efficient manner which cannot be accessed by unlicensed user which reduces data leakage.

References

[1] k. Dongre, R. S. Thakur, A. Abraham et al., "Secure cloud storage of data," in Computer Communication and Informatics (ICCCI), 2014 International Conference on. IEEE, 2014, pp. 1–5.

[2] Y. Shi, S. Abhilash, and K. Hwang, "Cloudlet mesh for securing mobile clouds from intrusions and network attacks," in The Third IEEE International Conference on Mobile Cloud Computing, Services, and Engineering,(Mobile Cloud 2015). IEEE, 2015.

[3] Alexsis Bell, Paul Rogers, Chris Farnell, Brett Sparkman, and Scott C. Smith,," Wireless Patient Monitoring System" 2014 Health Innovations and Point-of-Care Technologies Conference Seattle, Washington USA, October 8-10, 2014,pp.1-4

[4] Shruthi Ramdas , Ankitha K "Advanced Protection for Patient Information in Medical Database" IJCSMC, Vol. 6, Issue. 6, June 2017,pp. 1-11

[5] ANSI, ISO/TS 18308 Health Informatics-Requirements for an Electronic Health Record Architecture, ISO 2003.

[6] R. Bakker, B. Barber, R. Tervo-Pellikka, A.Treacher, (eds.), Communicating Health Information in an Insecure World, in: Proceedings of the Helsinki Working Conference. 43:1, 1995. 2.

[7] B. Barber, D. Garwood, P. Skerman, In: Security in Hospital Information Systems, Security and data protection programme presented at the IMIA WH10 Working conference, Durham. 1994.

[8] S. M. Furnell, P.W. Sanders, Security management in the health-care environment, in: R.A. Greenes, H.E. Peterson, D.J. Protti, (eds.), MEDINFO '95, Proceedings of the eighth World Congress on Medical Informatics. Canada. p. 675–678.

[9] A. Patel, I. Kantzavelou, Implementing network security guidelines in health-

care information systems. In: MEDINFO '95. Proceedings of the eighth World Congress on Medical Informatics. Vancouver Trade and Convention Centre, Canada. p. 671–674.